TECHNICAL REPORT AMR-SS-06-36

IPSEC VPN CAPABILITIES AND INTEROPERABILITY

Laurie Fraser
Kathryn Roose

System Simulation and Development Directorate
Aviation and Missile Research, Development, and Engineering Center

and

Greg Nix
SAIC, Inc.
6725 Odyssey Drive
Huntsville, AL 35806

July 2006

DESTRUCTION NOTICE

FOR CLASSIFIED DOCUMENTS, FOLLOW THE PROCEDURES IN DoD 5200.22-M, INDUSTRIAL SECURITY MANUAL, SECTION II-19 OR DoD 5200.1-R, INFORMATION SECURITY PROGRAM REGULATION, CHAPTER IX. FOR UNCLASSIFIED, LIMITED DOCUMENTS, DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENT.

DISCLAIMER

THE FINDINGS IN THIS REPORT ARE NOT TO BE CONSTRUED AS AN OFFICIAL DEPARTMENT OF THE ARMY POSITION UNLESS SO DESIGNATED BY OTHER AUTHORIZED DOCUMENTS.

TRADE NAMES

USE OF TRADE NAMES OR MANUFACTURERS IN THIS REPORT DOES NOT CONSTITUTE AN OFFICIAL ENDORSEMENT OR APPROVAL OF THE USE OF SUCH COMMERCIAL HARDWARE OR SOFTWARE.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 2006	Final

4. TITLE AND SUBTITLE
IPSec VPN Capabilities and Interoperability

5. FUNDING NUMBERS

6. AUTHOR(S)
Laurie Fraser, Kathryn Roose, and Greg Nix

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Commander, U.S. Army Research, Development, and Engineering Command
ATTN: AMSRD-AMR-SS-AE
Redstone Arsenal, AL 35898

8. PERFORMING ORGANIZATION REPORT NUMBER
TR-AMR-SS-06-36

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Advanced Prototyping, Engineering & eXperimentation (APEX) Laboratory at the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) supports many distributed simulation exercises utilizing the Defense Research Engineering Network (DREN). A mix of classified and unclassified simulation exercises have recently been held, utilizing the Type B Asynchronous Transfer Mode (ATM) services provided by the DREN. Upcoming unclassified experiments will involve participants that are on networks that peer with the DREN and will require the use of the DREN Type A (IP only) services. Thus the use of Internet Protocol Security (IPSec) Virtual Private Network (VPN) tunnels is being investigated as a means of providing a secure method of connectivity for these participants.

Two leading vendors that provide IPSec VPN services include Juniper (formerly Netscreen) and Cisco. Of interest is the interoperability of setting up an IPSec VPN tunnel with a Juniper Netscreen device on one end and a Cisco PIX device on the other. The focus of this work is to verify IPSec interoperability with no intent to compare PIX and Netscreen features. Also of interest is encapsulating Generic Routing Encapsulation (GRE) tunnels in the IPSec tunnel. A network lab has been set up and equipment borrowed to answer these questions, as well as determine effects upon latency in the AMRDEC simulation environment.

This report provides the results of this work, as well as configuration information and "lessons learned" during this effort.

14. SUBJECT TERMS
Internet Protocol Security (IPSec), Defense Research Engineering Network (DREN), Virtual Private Network (VPN), Generic Routing Encapsulation (GRE), simulation

15. NUMBER OF PAGES
26

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

ACKNOWLEDGEMENTS

Though not an editor on this technical report, contributions to this research were made by Eric Patterson during his employment with SAIC, Inc. Also, equipment and technical support from Cisco and Netscreen were graciously contributed to the efforts of this research.

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	EXPERIMENT PREMISE AND CONFIGURATION	2
III.	ANALYSIS PROCESS	8
IV.	PERFORMANCE RESULTS	8
V.	OBSERVATIONS	13
VI.	SUMMARY	13
	REFERENCES	15

LIST OF ILLUSTRATIONS

Figure	Title	Page
1.	List of Equipment	3
2.	Switch – System-to-System Environment	6
3.	Netscreen Homogeneous Environment	6
4.	Cisco Homogeneous Environment	7
5.	Cisco and Netscreen Heterogeneous Environment	7
6.	Ping Tests	8
7.	Nuttcp UDP Switch Test	9
8.	Nuttcp UDP Cisco-to-Cisco VPN Test	9
9.	Nuttcp UDP Netscreen-to-Netscreen VPN Test	10
10.	Nuttcp UDP Cisco-to-Netscreen Heterogeneous VPN Tests	10
11.	Nuttcp TCP Switch Test	11
12.	Nuttcp TCP Cisco-to-Cisco VPN Test	11
13.	Nuttcp TCP Netscreen-to-Netscreen VPN Test	12
14.	Nuttcp TCP Cisco-to-Netscreen Heterogeneous VPN Tests	12

LIST OF TABLES

Table	Title	Page
1.	IKE Phase I Parameters	3
2.	IKE Phase II Parameters	4
3.	Tunnel Configuration Step Overview	5

I. INTRODUCTION

The Aviation and Missile Research, Development, and Engineering Center (AMRDEC), located at Redstone Arsenal, Alabama, supports the Army's advanced simulated warfighting capabilities through direct simulation development and support, distributed simulation infrastructure, scenario development, and data collection and analysis from both a hardware engineering analytical perspective (hardware/firmware) as well as operations research. These capabilities are supported by the System Simulation and Development Directorate (SSDD).

To this end, the Advanced Prototyping, Engineering, and eXperimentation (APEX) Laboratory supports many distributed simulation exercises using the Defense Research Engineering Network (DREN). The APEX Laboratory is a research and development integration facility whose mission is to address the existing gap between warfighter simulation and engineering level simulation capabilities. This involves integrating the dynamics of doctrine, tactics, mobility, logistic support, Command, Control, and Communications (C3) decision-making, and human reaction in a synthetic battlefield driven by both tactical and technical constraints. The APEX Laboratory employs interoperable simulation technologies, such as Distributed Interactive Simulation (DIS) and High Level Architecture (HLA), to create an environment in which different representations of the battlefield are seamless or "transparent" to the participants. The APEX Laboratory provides a unique synergy of models, simulations, and prototype components in an unparalleled architecture to support Department of Defense (DOD) research and development activities.

Two experiments within the APEX Lab drove the requirement for this study: the Joint Aviation, Missile and Unmanned Systems (JAMUS) experiment and the Distributed Advanced Simulation for Helicopters (DASH). The JAMUS is an invitational event in which the community can integrate their respective models and simulations to address issues related to focus for that event. The focus for the first JAMUS was airspace management in a joint context. A series of these events will be held with a unique focus for each experiment.

The DASH provides unique challenges in that it is the result of collaboration between the AMRDEC and Defense Research and Development, Canada. Connecting the AMRDEC to a foreign lab presents security challenges above and beyond the scope (performance) of this report and is being studied individually. The DASH Test Bed will be located within the APEX Lab and will provide a high fidelity mission essential task load environment associated with aviation armed reconnaissance and attack missions. Once it is established, it will be used in experiments between the APEX Lab and DRDC-Valcartier to support the Canadian Multi-Mission Effects Vehicle (MMEV) exercise.

As noted, the APEX Laboratory at AMRDEC supports many distributed simulation exercises using the DREN. A mix of classified and unclassified simulation exercises have recently been held, using the Type B Asynchronous Transfer Mode (ATM) services provided by the DREN. Upcoming unclassified experiments will involve participants that are on networks that peer with the DREN and will require the use of the DREN Type A (Internet Protocol (IP) only) services. Thus the use of Internet Protocol Security (IPSec) Virtual Private Network (VPN)

tunnels is being investigated as a means of providing a secure method of connectivity for these participants.

Two leading vendors that provide IPSec VPN services include Juniper (formerly Netscreen) and Cisco. Of interest is the interoperability of setting up an IPSec VPN tunnel with a Juniper Netscreen device on one end and a Cisco PIX device on the other. The focus of this work is to verify IPSec interoperability with no intent to compare PIX and Netscreen features. Also of interest is encapsulating Generic Routing Encapsulation (GRE) tunnels in the IPSec tunnel. A network lab has been set up and equipment borrowed to answer these questions, as well as determine effects upon latency in the AMRDEC simulation environment.

II. EXPERIMENT PREMISE AND CONFIGURATION

The objective of this trial was two fold. The first objective was to look at the interoperability of two separate vendor implementations of IPSec VPN tunneling in an environment where both vendors play a role. The second objective was to determine some baseline statistics for the latency and max packet count that each piece of equipment could handle. In order to determine the interoperability of the systems, it was necessary to become proficient in building an encrypted tunnel between like devices.

In order to build an IPSec VPN tunnel, there is a process known as Internet Key Exchange (IKE). This process is critical for each device to understand that the request is genuine. IKE requires two phases for the secure VPN Tunnel to exist. These phases are as follows:

Phase I – Establish a Security Association

Phase II – Establish Tunnels or Endpoint Security Associations

Phase I is where the two endpoints exchange information concerning the type of encryption that will occur and exchange a unique pass key. If this fails between the two devices, then no tunnel or encrypted payloads will be exchanged and the IKE fails. There are debug tools that can be run on each system to show the details of this phase. If a failure occurs, the tools will show what the remote system was sending that may not be congruent with the established configuration.

Phase II is where the type and strength of encryption that will occur is matched up. Neither phase sets the remote device; it requires the information to match up properly for a functioning tunnel. This phase is where the type of encryption, encapsulation, and authentication is exchanged and established.

Once the two phases of IKE are complete, a functioning tunnel is available for traffic flow. Therefore, the understanding of matching information on like systems for the establishment of an IPSec VPN tunnel is accomplished. Figure 1 shows the equipment used to emulate two networks separated by an external network.

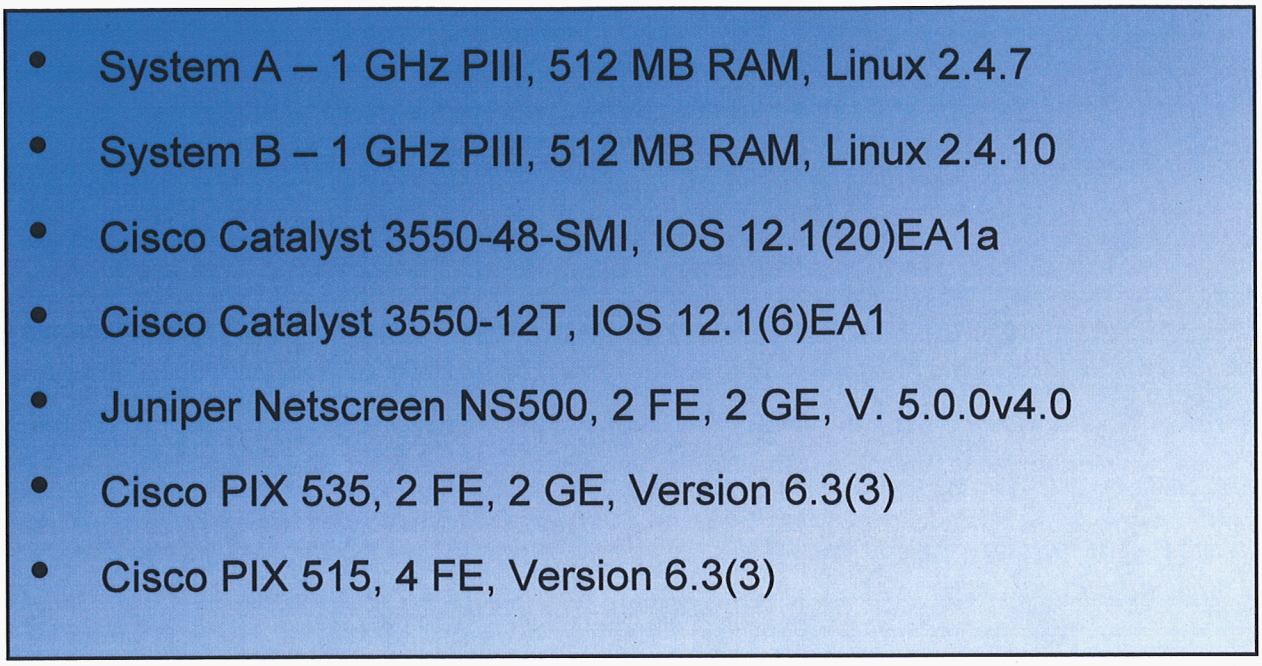

Figure 1. List of Equipment

Using the aforementioned equipment in a variety of configurations, homogenous and heterogeneous environments for testing purposes were created. The application of IKE and its two phases were critical in the understanding of how each manufacturer established the IPSec VPN tunnel. Cisco and Juniper/Netscreen follow the standard and were found to communicate with each other well; however, terminology differs between the two. In order for there to be clean communication between two sites using different hardware, these differences must be understood. Tables 1 and 2 depict the differences in terms for Phase I and Phase II of the setup. Once these variables are set equal to each other, the IKE works properly and a tunnel is established.

Table 1. IKE Phase I Parameters

Cisco	Juniper/Netscreen
Authentication	Method
Encryption	Encryption
DH Group	DH Group
Hash	Hash

Table 2. IKE Phase II Parameters

Cisco	Juniper/Netscreen
Diffie-Hellman Group (DH)	Perfect Forward Secrecy (PFS)
Encapsulation	Encapsulation
Encryption	Encryption
Hash	Authentication

In order to bring up the tunnel, a pre-shared key was used. Other methods such as Rivest, Shamir and Adelman (RSA) Certificates are available; however, as a certificate server was not accessible, a pre-shared key was used. This key is entered on the Gateway pages of each system and is specific to the remote system. In order to define the remote IP address, Cisco calls it "Peer IP," while Netscreen uses the term "Remote Gateway IP." It is important to understand all of these variances as they effect the configuration. The definition of interesting traffic is required for the initiation of the entire IKE process. This is usually the last step in the process as a reference back to the IKE policy in the definition of the path.

Once the completed IKE policies were in place, traffic was placed on the network and network monitoring was used for determining packet flow. Cisco provides an excellent web interface and graphics that monitor active IKE and IPSec VPN tunnels. When the Cisco PIX was in the mix, it was the method of choice for verifying the tunnel state. Using Etherel and Network Observer, it was determined that encrypted tunneling was occurring in the Wide Area Network (WAN) and verified the transmission rates reported in the results. An overview of the configuration steps to set up the tunnels on each of the devices is shown in Table 3.

Table 3. Tunnel Configuration Step Overview

Netscreen	Cisco PIX
• Zone Definitions • Interface Definitions • Router Table • Create Phase 1 Proposal • Phase 1 Table Information • Create Phase 2 Proposal • Phase 2 Table Information • Define Gateway to the Remote End • Apply Phase 1 Proposal to the Gateway • Define VPN • Apply Phase 2 Proposal to Interface • Ascertain IPSec VPN Tunnel Active	• Define Interfaces • Router Table • Definition of Pre-shared Keys • Create Phase 1 Proposal • Create Phase 2 Proposal • Application of Tunnel Policy to the Interface • Configure IPSec Rules • Monitor Tunnel to Ascertain It Is Active

Once the basic build of an IPSec VPN tunnel between the two devices was accomplished, it was important to fulfill the second objective: performance of the link. The environment of interest was that of broadcast and multicast traffic over the wide area. Due to the nature of this traffic, it is important that the tunnel is established and can accommodate the broadcast traffic generated.

Following are figures of the various configurations used for each set of the test data. Figure 2 depicts a system-to-system configuration on a switch to provide a base for comparisons. Figure 3 depicts the IPSec tunnel as built in a homogeneous Netscreen environment. Figure 4 depicts the tunnel as built in a homogeneous Cisco environment. Figure 5 depicts the tunnel as built in a heterogeneous Netscreen-to-Cisco environment.

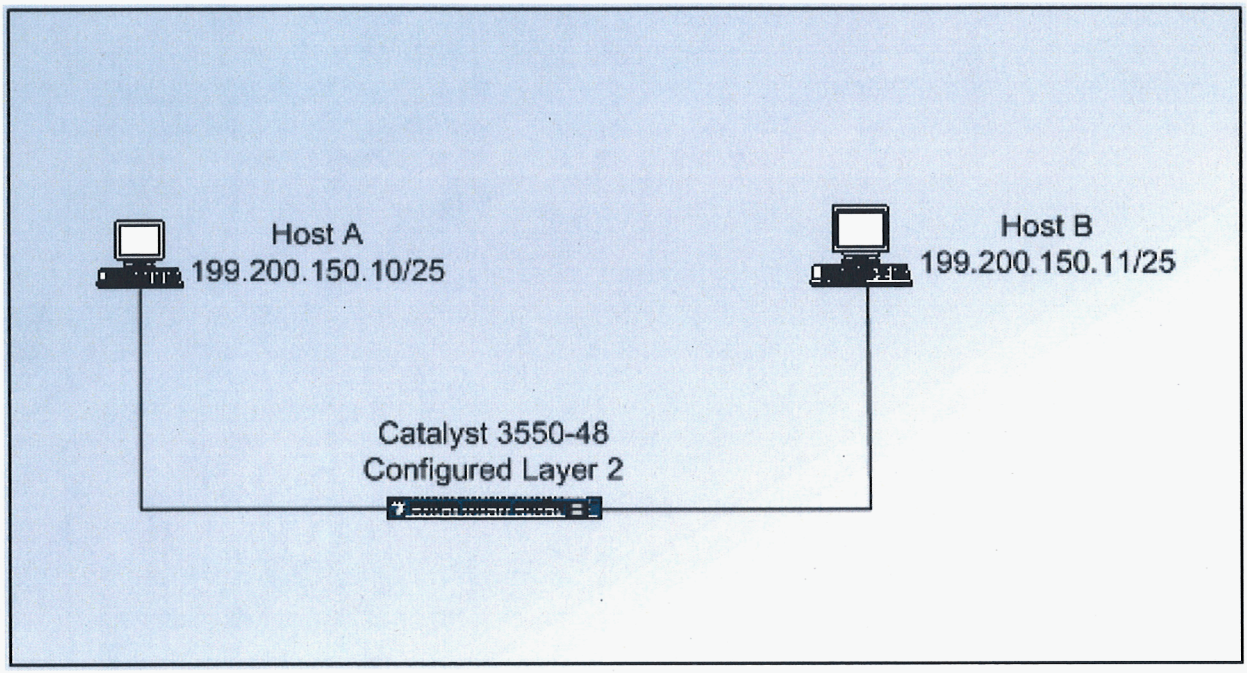

Figure 2. Switch – System-to-System Environment

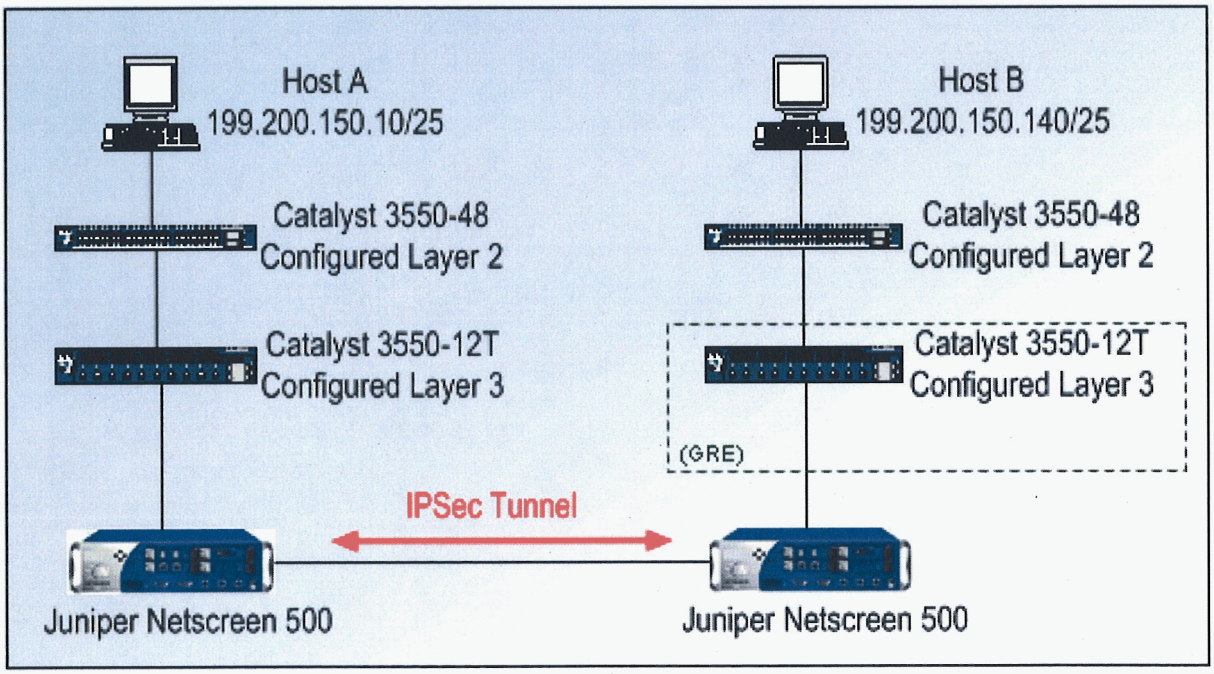

Figure 3. Netscreen Homogeneous Environment

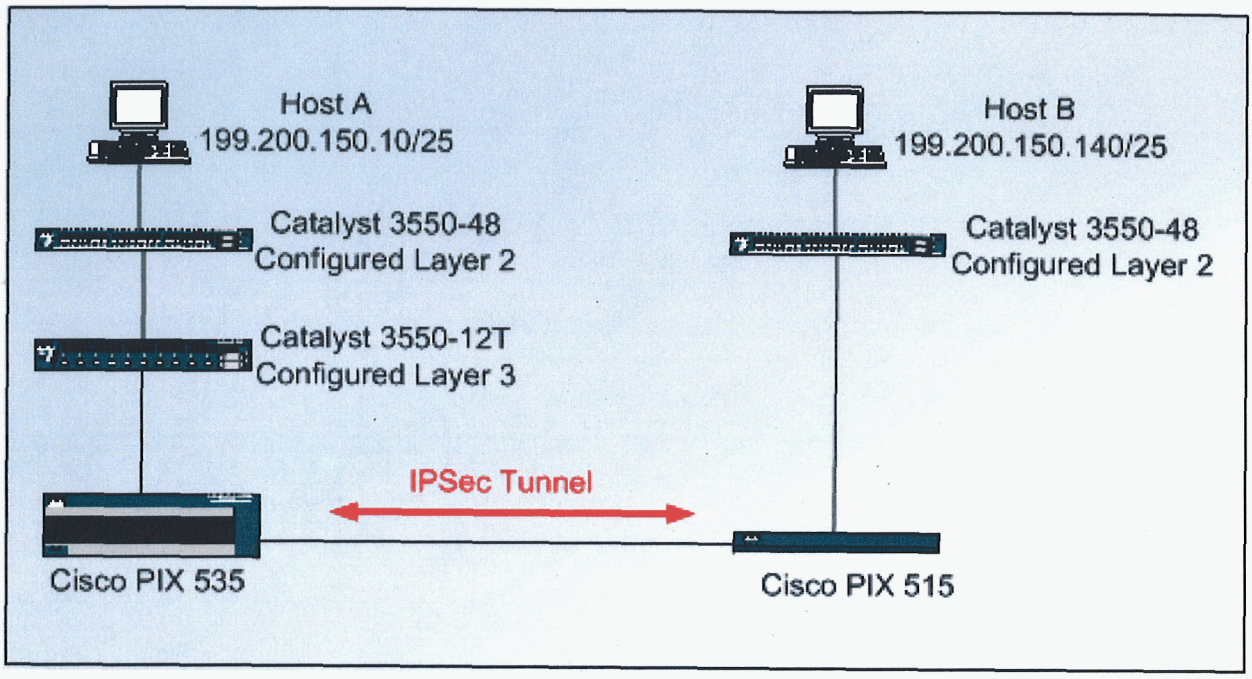

Figure 4. Cisco Homogeneous Environment

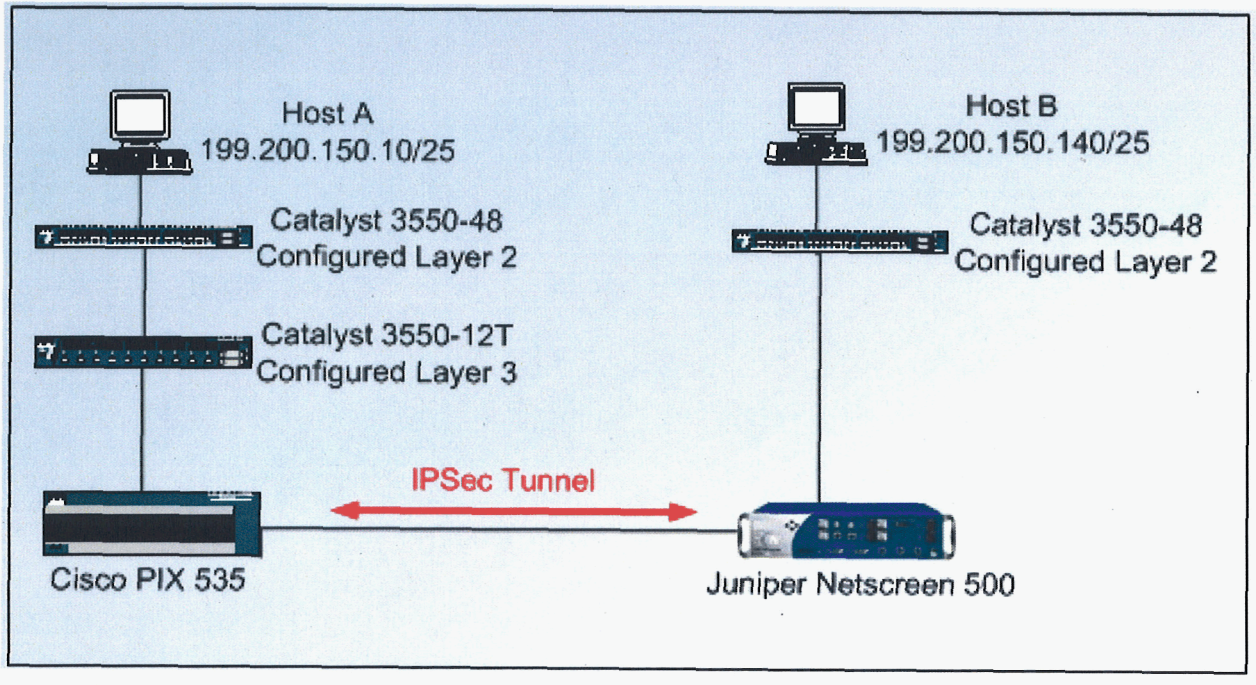

Figure 5. Cisco and Netscreen Heterogeneous Environment

III. ANALYSIS PROCESS

The tools to help in the analysis process of the configur(ations included the utility "ping," and "nuttcp." Ping was developed by Mike Muuss at the Army Research Laboratory (ARL). Ping was named after the sound sonar makes, inspired by the whole principle of echo-location. Ping uses timed IP/ICMP ECHO_REQUEST and ECHO_REQUEST packets to probe the distance to the target machine. Nuttcp is a tool developed by Bill Fink and Rob Scott. This tool is a network performance tool used to determine the raw Transport Control Protocol (TCP) or User Data Protocol (UDP) network layer throughput by transferring memory buffers from a source system across an interconnecting network to a destination system, either transferring data for a specified time interval or alternatively transferring a specified number of buffers. In addition to reporting the network throughput in Mbps, it also provides additional information related to the data transfer such as user, system and wall-clock time, transmitter and receiver CPU utilization, and loss percentage for UDP transfers.

IV. PERFORMANCE RESULTS

Figure 6 provides the result of ping tests from Host A and Host B for each configuration.

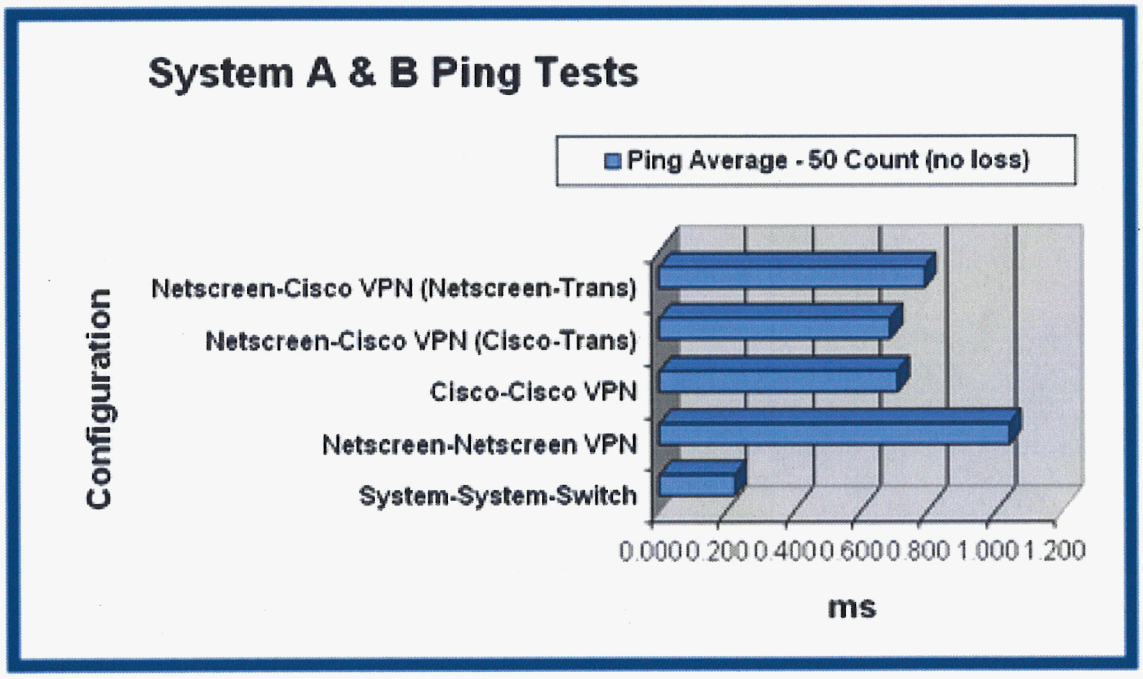

Figure 6. Ping Tests

The tests were averaged over a 50-count test. Also, the Netscreeen and Cisco VPN configuration was tested using each side as a transmitter. There was no loss of data in any of these tests, and the results appeared normal.

Figures 7 through 10 provide the results of the UDP nuttcp tests from Host A to Host B for the aforementioned configurations.

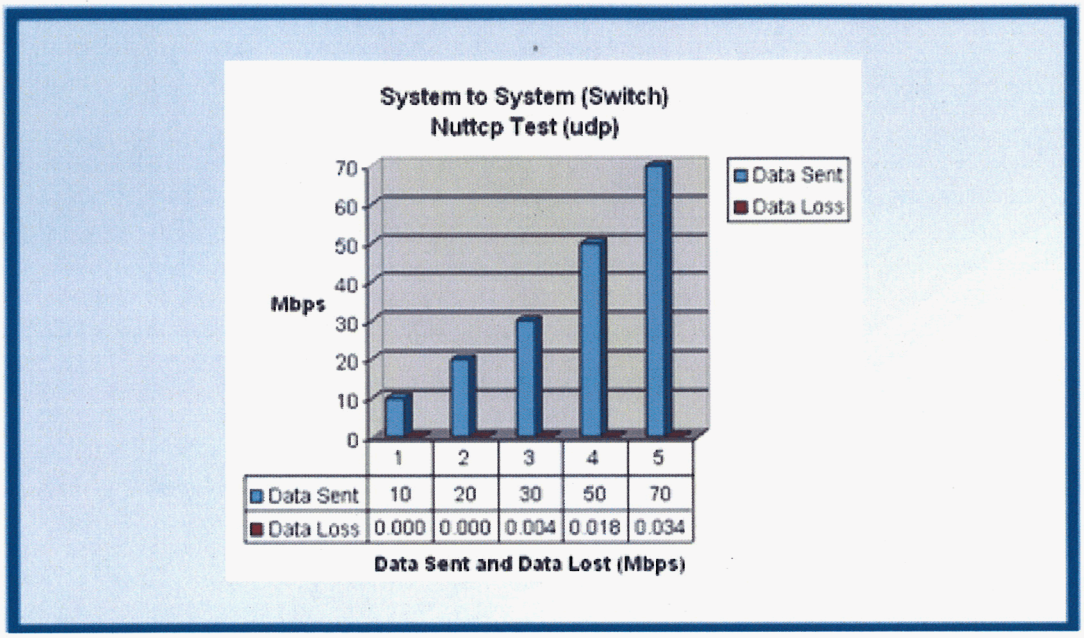

Figure 7. Nuttcp UDP Switch Test

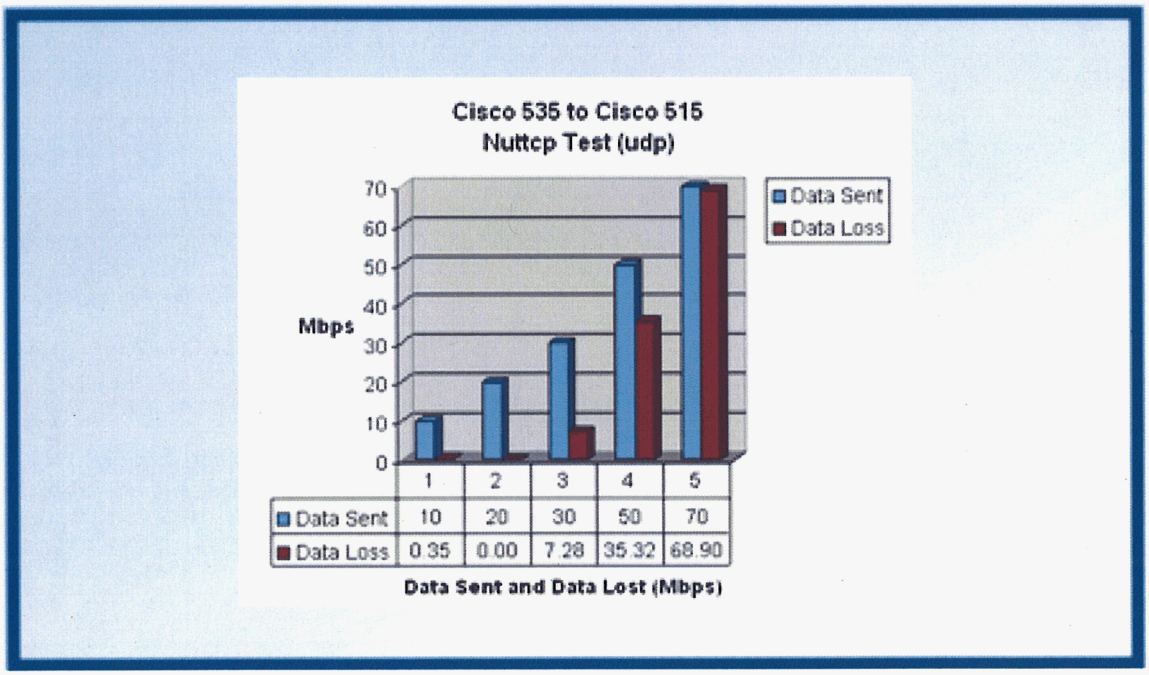

Figure 8. Nuttcp UDP Cisco-to-Cisco VPN Test

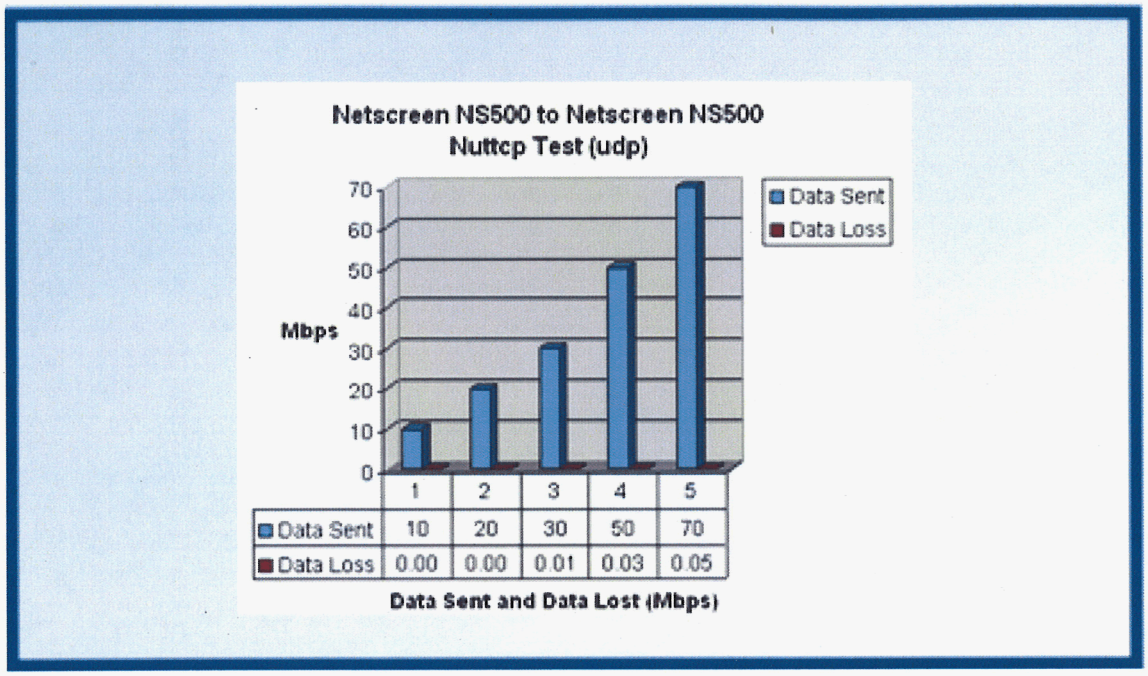

Figure 9. Nuttcp UDP Netscreen-to-Netscreen VPN Test

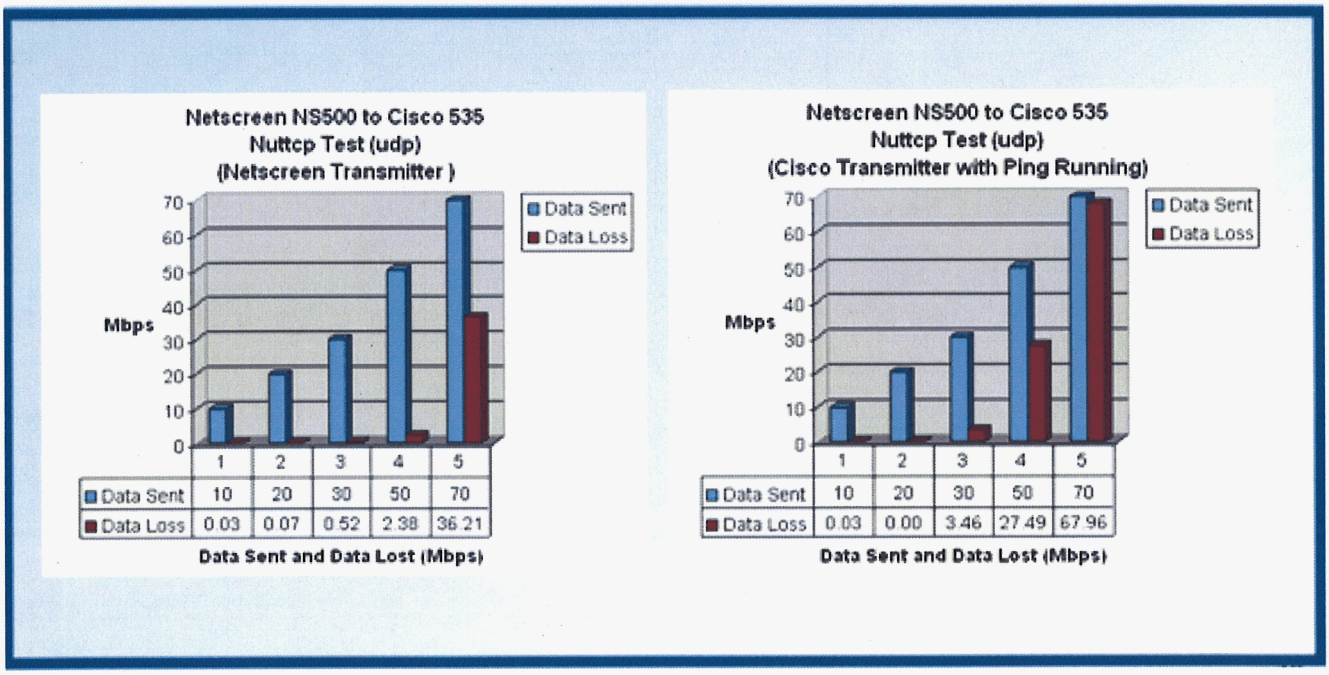

Figure 10. Nuttcp UDP Cisco-to-Netscreen Heterogeneous VPN Tests

The performance of the Netscreen device appeared to be more consistent. Data loss on the Cisco PIX was sustained after 20 Mbps of UDP traffic was passed.

Figures 11 through 14 provide the results of the TCP nuttcp tests from Host A to Host B for the aforementioned configurations.

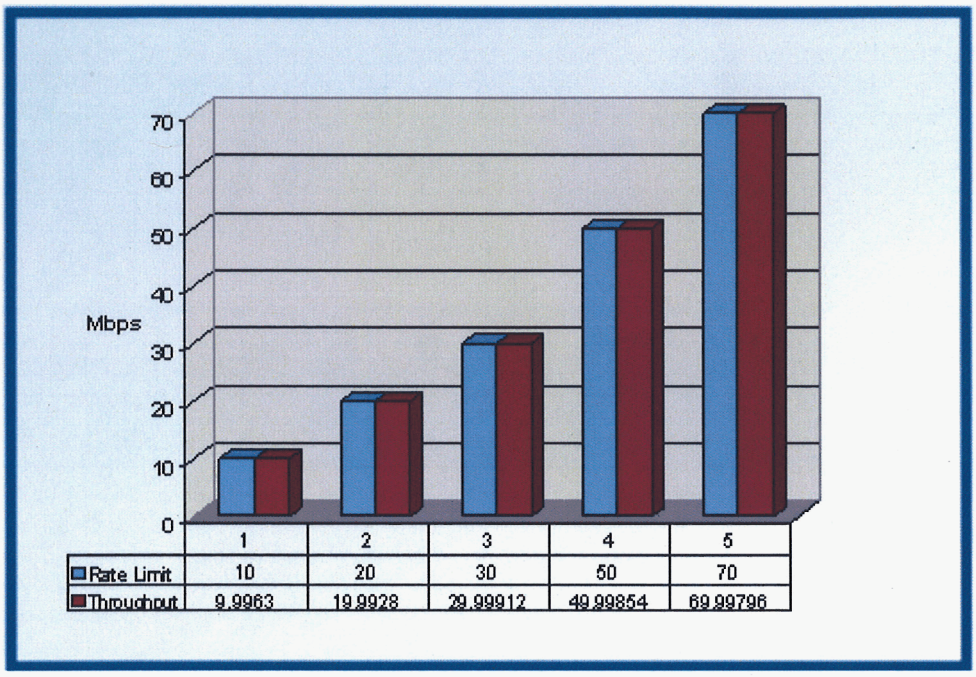

Figure 11. Nuttcp TCP Switch Test

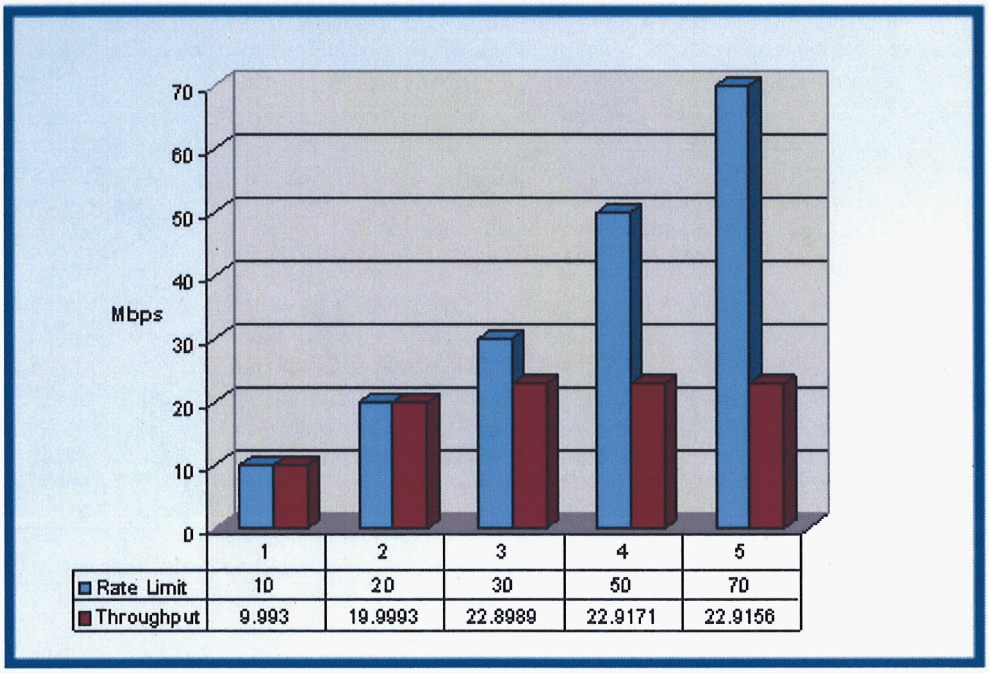

Figure 12. Nuttcp TCP Cisco-to-Cisco VPN Test

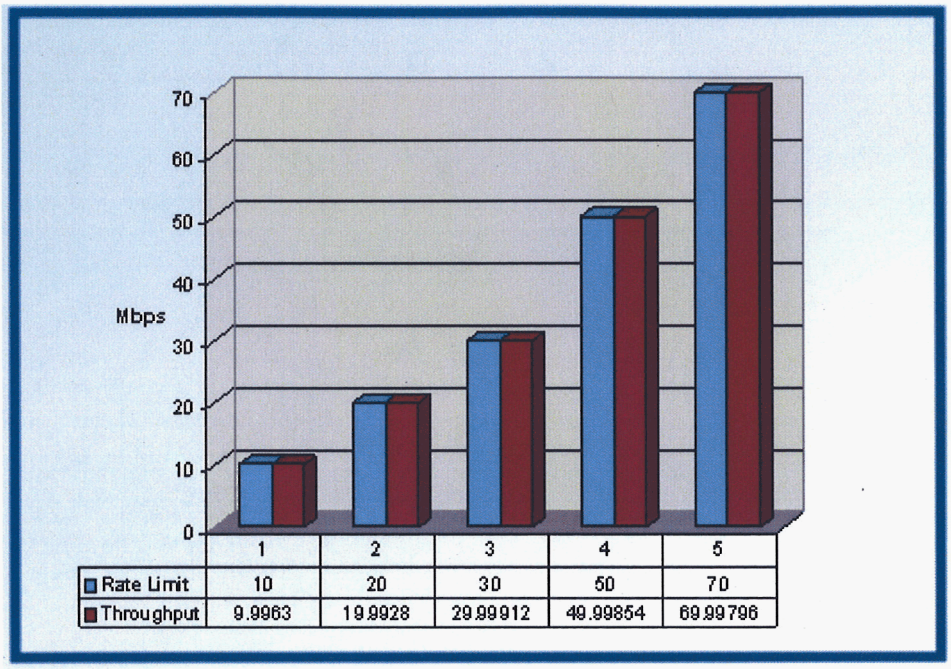

Figure 13. Nuttcp TCP Netscreen-to-Netscreen VPN Test

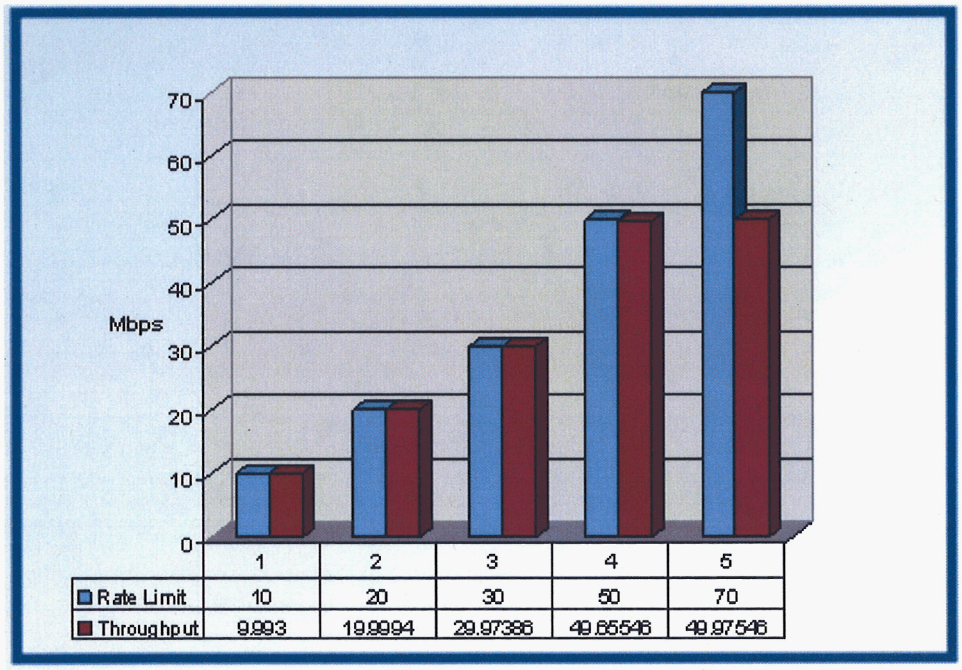

Figure 14. Nuttcp TCP Cisco-to-Netscreen Heterogeneous VPN Tests

The Cisco TCP throughput data shows that the PIX will sustain about 23 Mbps of throughput without loss. The loss of data exhibited in the Cisco UDP tests is consistent with the TCP throughput data tests.

V. OBSERVATIONS

The following observations were noted:

- Debugging is easier on the Cisco PIX due to the graphical monitoring capability.
- Netscreen offers more methods of authentication – Digital Signal Algorithm (DSA), RSA and Preshared Key. Cisco only offers RSA and Preshared Key.
- Cisco's web interface appears to be unstable, wherein the Netscreen interface was stable. However, the Cisco tools for verifying the establishment of the tunnel was much easier to use and more developed than those of Netscreen.
- Netscreen's configuration steps match the process, wherein Cisco's configuration steps include many shortcuts.
- Netscreen's performance appeared more consistent.
- The Cisco TCP throughput data shows that the PIX will sustain about 23 Mbps of throughput without loss.
- The loss in the Cisco UDP tests is consistent with the TCP throughput data.

VI. SUMMARY

This effort provided valuable insight into the performance characterization of the devices studied and also answered the question of interoperability of IPSec tunnels using equipment from major vendors. The use of IPSec tunnels for future architectures in the existing environment were found to be a viable option and will be given further study.

REFERENCES

1. *Cisco Secure PIX and NetScreeen Screen OS 2.5*, Netscreen.

2. *Configuring an IPSec LAN-to-LAN Tunnel Between the Cisco PIX Firewall and a NetScreeen Firewall*, http://www.cisco.com.

3. *Decoding IPSec*, Gail Meredith , *Second Qtr. 2002 Packet* – Cisco Systems.

4. *IPSec and IKE*, Juniper http://www.juniper.net/techpubs/software/junos/junos63/swconfig63-sys-basics/html/software-overview39.html#1045845.

5. *IPSec and MPLS: Which VPN is right for you ?,* Network Magazine http://www.networkmagazineindia.com/200203/200203focus1.shtml.

6. *Explained*, Carlos Cardenas, September 7, 2001, University of Texas at San Antonio, Computer Science Information Security Laboratory.

7. *IPSec/IKE Interoperability: Feedback from the IPSec 2001 Conference Demo*, www.hsc.fr.

8. *IPSec Tunnel Creation*, Chris Gutridge, March 1, 2003, SANS GSEC Practical version 1.4b option 1.

9. *IPSec Virtual Private Networks: A Technical Review*, Jim Tiller, Lucent Technologies, NetworkCare, 2000, htttp://www.lucent-networkcare.com.

10. NUTTCP – ftp://ftp.lcp.nrl.navy.mil/pub/nuttcp.

11. *Security Architecture for the Internet Protocol*, RFC 2401, http://www.ietf.org/rfc/rfc2401.txt?number=2401.

12. *Understanding IPSec*, Laura Taylor, Intranet Journal, 6/13/2, http://intranetjournal.com/articles/200206/pse_06_13_02a.html.

INITIAL DISTRIBUTION LIST

		Copies
Weapon Systems Technology Information Analysis Center ATTN: Ms. Vakare Valaitis 1901 N. Beauregard Street, Suite 400 Alexandria, VA 22311-1720		1
Defense Technical Information Center 8725 John J. Kingman Rd., Suite 0944 Fort Belvoir, VA 22060-6218		1
SAIC, Inc. ATTN: Lindsay Thompson/Greg Nix 6725 Odyssey Drive Huntsville, AL 35806-3301		1
AMSRD-AMR		(Electronic)
AMSRD-AMR-IN-IC		2
AMSRD-AMR-SS-AE,	Laurie Fraser	1
	Kathryn Roose	1
AMSRD-L-G-I,	Mr. Dayn Beam	1